ACQUISITION & TECHNOLOGY

THE WILL TO CHANGE

SYSTEM ASSURANCE

Minimizing Risks to Defense Systems

> The risk to DoD systems is rising with broadened use of commercial software products

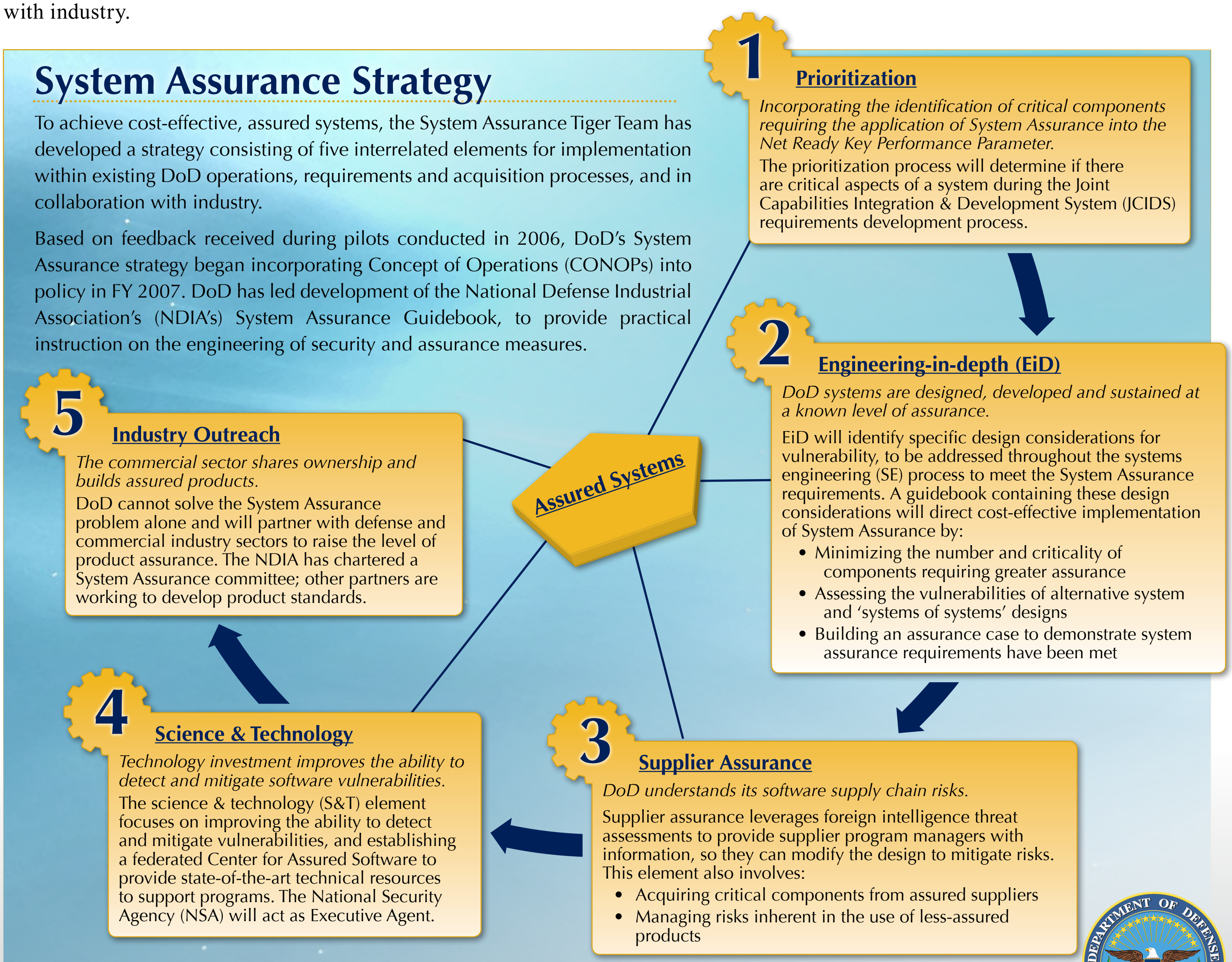
Most Department of Defense (DoD) capabilities depend on software developed in the commercial sector. Enemies of the United States including nation-states, terrorists, criminals, and rogue software developers, may damage or gain control of DoD systems through supply chain opportunities (intentionally embedding malicious code), or by remotely exploiting unintentionally vulnerable software. This risk is rising with broadened use of commercial products and increasing globalization of software development.

In 2004, DoD established a System Assurance Tiger Team to create a strategy to mitigate these risks. In 2005, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) and Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)), approved the strategy and tasked the Tiger Team with implementation, emphasizing the need for partnership with industry.

System Assurance Strategy

To achieve cost-effective, assured systems, the System Assurance Tiger Team has developed a strategy consisting of five interrelated elements for implementation within existing DoD operations, requirements and acquisition processes, and in collaboration with industry.

Based on feedback received during pilots conducted in 2006, DoD's System Assurance strategy began incorporating Concept of Operations (CONOPs) into policy in FY 2007. DoD has led development of the National Defense Industrial Association's (NDIA's) System Assurance Guidebook, to provide practical instruction on the engineering of security and assurance measures.



Assured Systems

1 **Prioritization**

Incorporating the identification of critical components requiring the application of System Assurance into the Net Ready Key Performance Parameter.

The prioritization process will determine if there are critical aspects of a system during the Joint Capabilities Integration & Development System (JCIDS) requirements development process.

2 **Engineering-in-depth (EiD)**

DoD systems are designed, developed and sustained at a known level of assurance.

EiD will identify specific design considerations for vulnerability, to be addressed throughout the systems engineering (SE) process to meet the System Assurance requirements. A guidebook containing these design considerations will direct cost-effective implementation of System Assurance by:

- Minimizing the number and criticality of components requiring greater assurance
- Assessing the vulnerabilities of alternative system and 'systems of systems' designs
- Building an assurance case to demonstrate system assurance requirements have been met

3 **Supplier Assurance**

DoD understands its software supply chain risks.

Supplier assurance leverages foreign intelligence threat assessments to provide supplier program managers with information, so they can modify the design to mitigate risks. This element also involves:

- Acquiring critical components from assured suppliers
- Managing risks inherent in the use of less-assured products

4 **Science & Technology**

Technology investment improves the ability to detect and mitigate software vulnerabilities.

The science & technology (S&T) element focuses on improving the ability to detect and mitigate vulnerabilities, and establishing a federated Center for Assured Software to provide state-of-the-art technical resources to support programs. The National Security Agency (NSA) will act as Executive Agent.

5 **Industry Outreach**

The commercial sector shares ownership and builds assured products.

DoD cannot solve the System Assurance problem alone and will partner with defense and commercial industry sectors to raise the level of product assurance. The NDIA has chartered a System Assurance committee; other partners are working to develop product standards.

If you would like to provide comments or suggestions, or if you would like more information:
Acquisition & Technology • http://www.acq.osd.mil/at • 703-571-9020